Lema do Bombeamento para Linguagens Regulares

* Linguagens que não são regulares

$B = \{0^n 1^n \mid n \geq 0\}$

requer que o AFD saiba contar

$C = \{w \mid w$ tem o mesmo número de 0's e 1's$\}$

→ um AFD não consegue contar uma quantidade arbitrária.

→ Ex: $\hat{\delta}(q_0, w) = S_{i,j} \iff w$ contém i 0's e j 1's

$$Q = \{S_{i,j} : i, j \geq 0\}$$

infinito

$D = \{w \in \{0,1\}^* :$ w tem o mesmo número de subcadeias "01"s e "10"s $\}$

A linguagen D é regular

⚠ Pode ser que a sua modelagem esteja ruim e que seja possível fazer com um número finito de estados.

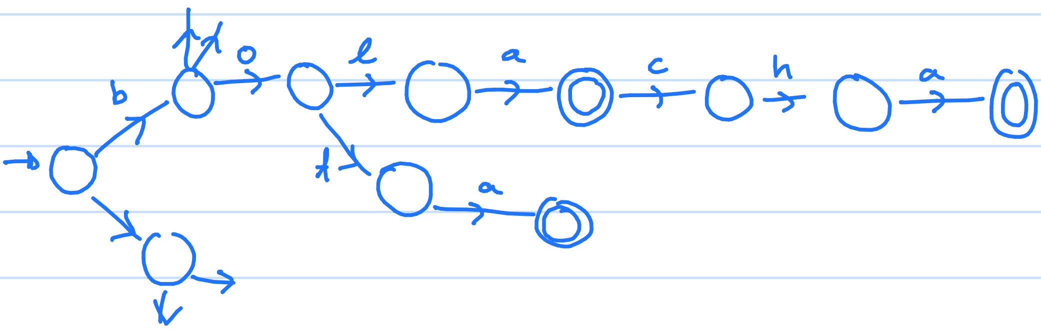
- Como podemos provar com toda certeza que uma linguagem ñ é regular?

R: Lema do Bombeamento.

Cadeias vs Números de Estados

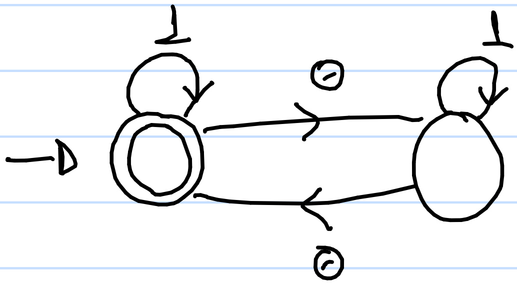
- Toda linguagem que possui um # finito de cadeias é regular

Ex: L é a linguagem que contém toda as palavras da língua portuguesa



- Como pode existir linguagens regulares com um # infinito de cadeias?

Ex: $L = \{ w \in \{0,1\}^* \mid w \text{ contém um \# par de 0's} \}$



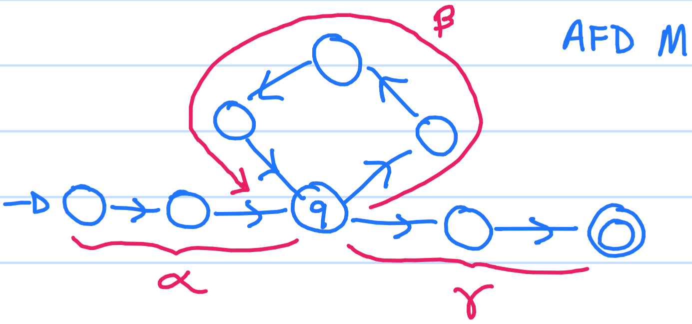
Qual a maior cadeia que um AFD com n estados pode aceitar sem usar um ciclo?

R: $n-1$ => Se w é um cadeia da linguagem e $|w| \geq n$, então a sequência de aceitação de w contém um ciclo.

Ideia Chave

Se você pode seguir o ciclo uma vez, então você pode segui-lo quantas vezes quiser e continuar dentro da linguagem

$\omega = \alpha\beta\gamma$



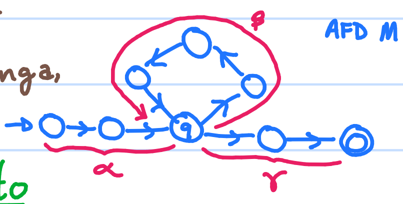
- $\omega \in L(M)$
- $\alpha\beta\beta\gamma \in L(M)$
- $\alpha\beta\beta\beta\gamma \in L(M)$
- $\alpha\beta\beta\beta\cdots\beta\gamma \in L(M)$
- $\alpha\gamma \in L(M)$

NOTA: toda cadeia da forma $\omega = \alpha\beta^i\gamma \in L(M)$ para $i \geq 0$

O que podemos dizer ser verdadeiro?

$\omega = \alpha\beta\gamma$

Se a linguagem for regular e ω for suficientemente longa, i.e., $|\omega| \geq p$, → comprimento de bombeamento



↳ Longo o suficiente para força toda cadeia ter um ciclo.

Então $\omega = \alpha\beta\gamma$ tal que

(1) $\alpha\beta^i\gamma$ pertence à linguagem, para $i \geq 0$.

(2) $|\beta| > 0$ → o ciclo precisa de ao menos um arco

(3) $|\alpha\beta| \leq p$ → o ciclo acontece no "começo"

0,1 $p=2$

$$w = \overbrace{q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2, \dots, q_i}^{\alpha}, \overbrace{q_{i+1}, \dots, q_{j-1}, q_j}^{\beta}, q_{j+1}, \dots, q_k$$

$q_i = q$, $q_j = q$

$\rightarrow$ $q_0 \dots q_{j-1}$ são estados distintos

$\Rightarrow j-1 < p \Rightarrow j \leq p$

$$|\alpha\beta| = j \leq p$$

O que descobrimos?

Se uma linguagem é regular, então existe um comprimento (comprimento de bombeamento) tal que toda cadeia de comprimento maior do que p podem ser "bombeada".

- Esse comprimento de bombeamento é uma propriedade da linguagem!

Lema do Bombeamento

Se L é uma linguagem regular, então L tem um comprimento p tal que qualquer cadeia $w \in L$, com $|w| \geq p$, pode ser escrita como

$$w = \alpha\beta\gamma$$

tal que as seguintes condições valem

(1) $\alpha\beta^i\gamma \in L$, para todo $i \geq 0$

(2) $|\beta| > 0$

(3) $|\alpha\beta| \leq p$

Roteiro para demonstrar que L não é regular

- Suponha, para uma contradição, que L não é regular
- Seja p o comprimento de bombeamento de L
- Qualquer cadeia de comprimento maior que p pode ser bombeada
- Escolha uma cadeia $w \in L$, $|w| \geq p$, que seja conveniente
- Mostre que $w = \alpha\beta^i\gamma$ não pertence à L, para algum $i \neq 1$, independentemente de quem seja α, β, γ.

$$w = \underbrace{w_1\, w_2\, w_3\, w_4}_{\alpha}\ \underbrace{w_5\, w_6}_{\beta}\ \underbrace{w_7\, w_8\, w_9\, w_{10}}_{\gamma}$$

$$w = \underbrace{w_1\, w_2\, w_3\, w_4\, w_5\, w_6\, w_7}_{\alpha}\ \underbrace{w_8\, w_9\, w_{10}}_{\beta} \qquad \gamma = \varepsilon$$

$$w = \underbrace{w_1\, w_2\, w_3}_{\alpha}\ \underbrace{w_4\, w_5\, w_6\, w_7}_{\beta}\ \underbrace{w_8\, w_9\, w_{10}}_{\gamma}$$

- Conclua que w não pode ser bombeada

$\Rightarrow$ L não é regular!

$\boxed{\text{Exercício}}$

Prove que a linguagem $B = \{0^n 1^n \mid n \geq 0\}$ não é regular.

$w = 0^p 1^p$ $\qquad\qquad$ $p = 7$

Caso 1: $w = 0\,0\,0\,\underbrace{0\,0\,0}_{\beta}\,0\,1\,1\,1\,1\,1\,1\,1$

Caso 2: $w = 0\,0\,0\,0\,0\,\underbrace{0\,0\,1\,1}_{\beta}\,1\,1\,1\,1\,1$

Caso 3: $w = 0\,0\,0\,0\,0\,0\,0\,1\,\underbrace{1\,1\,1\,1}_{\beta}\,1\,1$

Caso 1: $w = 0\,0\,0\,\underbrace{0\,0\,0}_{\beta}\,0\,1\,1\,1\,1\,1\,1\,1$

$w = 0\,0\,0\,\underbrace{0\,0\,0}_{\beta}\,\underbrace{0\,0\,0}_{\beta}\,0\,1\,1\,1\,1\,1\,1\,1$

$$\alpha\beta^2\gamma = \alpha\beta\beta\gamma \notin B$$

Caso 2: $w = 0\,0\,0\,0\,0\,\underbrace{0\,0\,1\,1}_{\beta}\,1\,1\,1\,1\,1$

$w = 0\,0\,0\,0\,0\,\underbrace{0\,0\,1\,1}_{\beta}\,\underbrace{0\,0\,1\,1}_{\beta}\,1\,1\,1\,1\,1$

$$\alpha\beta^2\gamma = \alpha\beta\beta\gamma \notin B$$

Caso 3:

$$w = 0\,0\,0\,0\,0\,0\,0\,1\,\underbrace{1\,1\,1\,1}_{\beta}\,1\,1$$

$$w = 0\,0\,0\,0\,0\,0\,0\,1\,\underbrace{1\,1\,1\,1}_{\beta}\,\underbrace{1\,1\,1\,1}_{\beta}\,1\,1$$

$$\alpha\beta\beta\gamma \notin B$$

Exercício

Prove que a linguagem $B = \{0^n 1^n \mid n \geq 0\}$ não é regular.

Demonstração

- Suponha, para uma contradição, que B é regular.
- Pelo lema do bombeamento, B possui um comprimeto de bombeamento, que chamaremos de p.
- Seja $w = 0^p 1^p$ e note que $w \in B$.
- Pelo lema do bombeamento, w pode ser escrita como $w = \alpha\beta\gamma$ tal que as seguintes condições são válidas:

① $\alpha\beta^i\gamma \in B$, para todo $i \geq 0$

② $|\beta| > 0$

③ $|\alpha\beta| \leq p$

- Por ③, $|\alpha\beta| \leq p$, e como $w = 0^p 1^p$, temos que $\alpha\beta \in \{0\}^*$
- Portanto a soma do total de 0's e 1's nas cadeias α, β, γ é igual.
- Por ②, $|\beta| > 0$.

Logo, $s = \alpha\beta^2\gamma = \alpha\beta\beta\gamma \notin B$, contradição a ①. ■

Exercício

Prove usando o lema do bombeamento que a linguagem

$$C = \{ w \in \{0,1\}^* : |w|_0 = |w|_1 \}$$

ñ é regular.

Demonstração

- Seja p o comprimento de bombeamento de C.
- Seja $w = (01)^p$

$$\alpha = \varepsilon \quad \underbrace{01}_{\beta}\underbrace{01\,01\,01\,01}_{\gamma}$$

$\alpha \beta^i \gamma \in C$, para todo $i \geq 0$

escolhemos mal nossa cadeia w

Vamos tenta essa:

$$w = 0^p 1^p = \overset{1\,2\,3}{0000}\cdots\overset{p}{0}\,\overset{1\,2\,3}{111}\cdots\overset{p}{1}$$

Exercício

Mostre, usando o lema do bombeamento, que a linguagem

$$F = \{ zz \ : \ z \in \{0,1\}^* \}$$

não é regular.

Demonstração

- Suponha, para uma contradição, que F é regular
- Seja p o comprimento de bombeamento de F.
- Seja $z = 0^p 1$ e $w = zz = 0^p 1 0^p 1$.
- Claramente, $w \in F$.
- Como $|w| \geq p$, pelo lema do bombeamento, $w = \alpha\beta\gamma$, onde α, β, γ satisfazem as 3 propriedades do lema.
- Por ③, sabemos que $|\alpha\beta| \leq p$

$$w = \overbrace{\overset{1}{0}\,\overset{2}{0}\,\overset{3}{0}\,0\,0\,0 \cdots \overset{p}{0}\,1}^{z}\overbrace{0\,0\,0 \cdots 0\,1}^{z}$$

$$\alpha\beta$$

- Assim, $\alpha\beta \in \{0\}^*$.
- Por ②, $|\beta| \geq 1$
- Dada uma cadeia $y \in \{0,1\}^*$ tal que $y = a_1 a_2 a_3 \cdots a_{2n}$, definimos o meio da cadeia y, denotado por $m(y)$, como sendo n. Definimos também as notações y_E e y_D para denotar as seguintes subcadeias de y

$$y_E = a_1 a_2 \cdots a_n$$

$$y_D = a_{n+1} a_{n+2} \cdots a_{2n}$$

Assim $y = y_E y_D$

- Note que $m(y)$ é o índice do último símbolo de y_E e que $y \in F$ sse $y_E = y_D$

Levei mais de 10 minutos pensando em uma notação boa

Note o que estou fazendo aqui: estou inventando nomes e notação para me expressar melhor e conseguir escrever a prova

- Seja $w' = \alpha\beta^2\gamma$ e note que, por ① do lema do bombeamento, temos que $w' \in F$

uma contradição

- Note que $|w'| = |w| + |\beta| = 2(p+1) + |\beta|$.
- Se $|\beta|$ for ímpar, então $|w'|$ é ímpar e, portanto, $w' \notin F$.
- Assim, $|\beta|$ é par e existe um $k \in \mathbb{N}$ tal que $|\beta| = 2k$.
- Como $|\alpha\beta| \leq p$ e $w = 0^p 1 0^p 1$, temos que $w' = \alpha\beta^2\gamma$ contém um prefixo $\phi \in \{0\}^*$ de tamanho $p + |\beta|$
- Note que

$$m(w') = \frac{|w'|}{2} = \frac{2(p+1) + |\beta|}{2} = \frac{2(p+1) + 2k}{2} = p+1+k$$

- Por fim, note que $p + 2k \geq p+1+k \iff k \geq 1$

e sabemos que $k \geq 1$ pq sabemos que $|\beta| = 2k$ e $|\beta| > 0$

Vale pq $k \geq 1$

- Assim, $|\phi| = p + |\beta| = p + 2k \geq p+1+k = m(w')$
- Isso mostra que $w_e \sqsubseteq \phi$ e, por conseguinte, $w_e \in \{0\}^*$.
- Como $1 \sqsupseteq w'_d$, temos que $w'_e \neq w'_d$ e, consequentemente, $w' \notin F$, um absurdo. $\square$

Agora sim... a prova ficou show!

NoTa:

Observe que você não teria sucesso com a resolução do exercício se tivesse escolhido a cadeia $0^p 0^p$

Usando o Lema do Bombeamento p/ Sugar

$\boxed{\text{Exercício}}$

Prove, usando o lema do bombeamento, que a seguinte linguagem é regular.

$$E = \{ 0^i 1^j : i > j \}$$

$i = 7 \qquad j = 6$

$$00\underbrace{00000}_{\beta}\,111111$$

$|\alpha\beta| \leq p$

(1) $\alpha\beta^i\gamma$ pertence à linguagem, para $i \geq \underset{=0}{0}$.

$i = 0 \Rightarrow \alpha\gamma \in F$

$$0^{p+1}1^p = 0\ 0\ \underbrace{0\ 0\ 0}_{\beta}\ 1\ 1\ 1\ 1$$

$p = 4$

Demonstração

- $w = 0^{p+1} 1^p$
- $|w| \geq p \Rightarrow$ vale o lema do bombeamento p/ w
  - $\to$ Seja $w = \alpha\beta\gamma$ dado pelo lema
  - $\to$ Por ③, $|\alpha\beta| \leq p \Rightarrow \alpha\beta \in \{0\}^*$
  - $\to$ Por ②, $|\beta| \geq 1$
  - $\to$ $\alpha\gamma$ tem pelo menos um zero a menos do que $\alpha\beta\gamma = w$.
  - $\to$ Como w tinha exatamente um 0 a mais do que 1's, temos que $\alpha\gamma = 0^a 1^b$, onde $a \leq b$
  - $\to$ Assim, $\alpha\gamma \notin F$, contradição. ■

Exercício

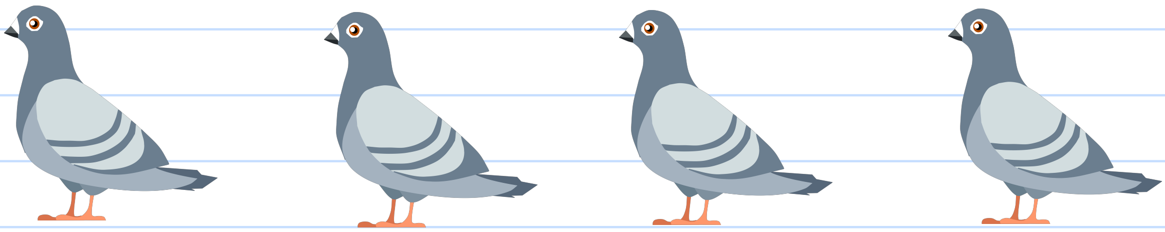
Prove, usando as propriedades regulares, que a seguinte linguagem não é regular.

$$C = \left\{ w \in \{0,1\}^* : \begin{array}{l} w \text{ contém o mesmo número de} \\ 0\text{'s e } 1\text{'s} \end{array} \right\}$$

Demonstração

- Sabemos que $B = \{0^n 1^n \mid n \geq 0\}$ ñ é regular.
- Suponha por contradição que C é regular
- Note que $B = C \cap \boxed{0^* 1^*}$ → é regula
- Como as linguagens regulares são fechadas sob a operação de interseção, temos que B é regular, uma contradição ∎

Princípio da Casa dos Pombos



Princípio da Casa dos Pombos

Se você colocar n pombos em um número de casas menor do que n, então uma casa terá pelo menos dois pombos

O que o princípio não diz:

Existe uma casa com exatamente dois pombos.

Lema do Bombeamento

Se L é uma linguagem regular, então L tem um comprimento p tal que qualquer cadeia $w \in L$, com $|w| \geq p$, pode ser escrita como

$$w = \alpha\beta\gamma$$

tal que as seguintes condições valem

(1) $\alpha\beta^i\gamma \in L$, para todo $i \geq 0$

(2) $|\beta| > 0$

(3) $|\alpha\beta| \leq p$

Demonstração

- Seja $M = (Q, \Sigma, \delta, q_0, F)$ um automato finito determinístico que reconhece a linguagem L e seja $p = |Q|$
- Seja $w = w_1 w_2 \cdots w_m$ uma cadeia tal que $w \in L$ e $|w| \geq p$.
- Seja $Q = \{q_0, q_1, \dots, q_n\}$ e seja $q_{r_0}, q_{r_1}, q_{r_2}, \dots, q_{r_m}$ a sequência de estados percorridos por M ao processar a cadeia w, i.e., $\hat{\delta}(q_0, w_1 w_2 \cdots w_i) = q_{r_i}$ para todo $i = 1, \dots, m$
- Essa sequência tem $m+1$ estados, logo, pelo princípio da casa dos pombos, existe um estado $q_t \in Q$ que aparece ao menos duas vezes na sequência.
- Dentre os estados que aparecem ao menos duas vezes na sequência, seja q_{r_j} o estado com o menor valor de j a aparecer uma segunda vez na sequência (o primeiro estado a aparecer repetido)
- Seja q_{r_k} a primeira aparição do estado q_{r_j} na sequência. Logo $k < j$.
- Seja $q_{r_k} = q_{r_j} = q_t$

todos distintos

1º repetição

$$\underbrace{q_0 = q_{r_0}, q_{r_1}, q_{r_2}, \dots, q_{r_k}, q_{r_{k+1}}, \dots,}_{\text{todos distintos}} \; q_{r_j}, q_{r_{j+1}}, \dots, q_{r_m}$$

$$q_{r_k} = q_t \qquad q_{r_j} = q_t$$

- Sejam $\alpha, \beta, \gamma \in \Sigma^*$ tais que

$$\hat{\delta}(q_0, \alpha) = q_{r_k}$$
$$\hat{\delta}(q_{r_k}, \beta) = q_{r_j}$$
$$\hat{\delta}(q_{r_j}, \gamma) = q_{r_m}$$

- Assim $\omega = \alpha\beta\gamma$
- Note que $\hat{\delta}(q_0, \alpha) = q_{r_k} = q_t$

$$\hat{\delta}(q_t, \beta) = \hat{\delta}(q_{r_k}, \beta) = q_{r_j} = q_t$$

$$\hat{\delta}(q_t, \gamma) = \hat{\delta}(q_{r_j}, \gamma) = q_{r_m}$$

- Como $r_k < r_j$, nos sabemos que $\beta \neq \varepsilon$ e, portanto, $|\beta| > 0$. Isso prova o item 2
- Como $m \geq p$ e p é o número de estados de M, e há $p+1$ estados na sequência $q_{r_0}, q_{r_1}, q_{r_2}, \dots, q_{r_p}$, temos que existe um estado repetido nesse prefixo da sequência $q_{r_0}, q_{r_1}, q_{r_2}, \dots, q_{r_p}, \dots, q_{r_m}$. Isso implica que $j \leq p$.
- Como $\hat{\delta}(q_0, \alpha\beta) = \hat{\delta}(\hat{\delta}(q_0, \alpha), \beta)$

$$= \hat{\delta}(q_{r_k}, \beta) = q_{r_j},$$

temos que $|\alpha\beta| = j \leq p$ (com isso concluímos 3)

- Agora vamos mostrar que 1 vale fazendo uma prova por indução em i.
- Primeiro, note que se $\omega \in L$, então $q_{r_m} \in F$
- Na realidade, precisaremos provar algo mais forte, vamos provar por indução o seguinte: $\alpha\beta^i\gamma \in L$ para todo $i \geq 0$ e $\hat{\delta}(q_0, \alpha\beta^i) = q_t$

Base: $i = 0$

- Então, precisamos mostrar que $w' = \alpha\gamma \in L$
- Note que

$$\hat{\delta}(q_0, \alpha\gamma) = \hat{\delta}(\hat{\delta}(q_0, \alpha), \gamma)$$
$$= \hat{\delta}(q_{r_k}, \gamma)$$
$$= \hat{\delta}(q_{r_j}, \gamma) = q_{r_m}$$

e

$$\hat{\delta}(q_0, \alpha\beta^0) = \hat{\delta}(q_0, \alpha\varepsilon) = \hat{\delta}(q_0, \alpha) = q_{r_k} = q_t$$

- Portanto, a base é válida.

- Passo

- Agora, suponha que $i > 0$ e que $\alpha\beta^{\gamma}\gamma \in L$ e $\hat{\delta}(q_0, \alpha\beta^{\gamma}) = q_t$ para qualquer $\gamma < i$
- Primeiro, note que

$$\hat{\delta}(q_0, \alpha\beta^i) = \hat{\delta}(\hat{\delta}(q_0, \alpha\beta^{i-1}), \beta)$$
$$= \hat{\delta}(q_t, \beta) = q_t$$

- Por fim, veja que

$$\hat{\delta}(q_0, \alpha\beta^i\gamma) = \hat{\delta}(\hat{\delta}(q_0, \alpha\beta^i), \gamma)$$
$$= \hat{\delta}(q_t, \gamma) = q_{r_m}$$

$\square$